Assessment Report: QSD 2004-87

United States Department of Energy
Nuclear Energy – Idaho Operations Office

Assessment of Safety System Software

and

Firmware at

Idaho National Engineering and Environmental Laboratory

Idaho Nuclear Technology and Engineering Center

Conducted April 26th, through April 29, 2004

Assessment of Safety System Software

and

Firmware at

Idaho National Engineering and Environmental Laboratory

Idaho Nuclear Technology and Engineering Center

Prepared by:

R.L. Blyth, NE-ID — May 26, 2004 Date

E. F. Branagan Jr., NE-70 — May 26, 2004 Date

Table of Contents

ACRONYMS

BBWI	Bechtel BWXT Idaho
CSCCB	Computer System Change Control Board
CSCF	Computer System Change Form
DMCS	Document Management and Control System
DNFSB	Defense Nuclear Facility Safety Board
ESF	Engineered Safety Feature
INEEL	Idaho National Environmental Engineering Laboratory
INTEC	Idaho Nuclear Technology and Engineering Center
LGWDCS	Liquid/Gaseous Waste Distributed Control System
NE-ID	Office of Nuclear Energy, Idaho Operations Office
M & O	Management and Operating
MCP	Management Control Procedure
PCU	Process Control Unit
PDD	Program Description Document
PEW	Process Equipment Waste
PLN	Plan
PRD	Program Requirements Document
PSD	Plant Safety Document
QA	Quality Assurance
SDD	System Design Description
SQA	Software Quality Assurance
SSCs	Structures, Systems and Components
TS	Technical Specifications/Standards
URL	Uniform Resource Locator or Identifier
V&V	Verification and Validation

INTRODUCTION

The purpose of the assessment was to assess safety system, instrumentation & control software at the Idaho National Engineering and Environmental Laboratory (INEEL). The assessment addressed two objectives:

1. Meet Commitment 4.2.3.3 of DOE Implementation Plan (IP) for DNFSB Recommendation 2002-1;

2. Assess the reliability and robustness of a Safety Class & Safety Significant Instrumentation & Control software system at INEEL.

In 1949 the U.S. Atomic Energy commission established the National Reactor Testing Station for testing various types of nuclear reactors and associated equipment. It is located in southeastern Idaho containing roughly 890 square miles at an average elevation of 4850 feet above sea level. Several name changes later it is now known as the INEEL.

The Idaho Nuclear Technology and Engineering Center (INTEC) is located on the INEEL. The facility was originally designed as a spent nuclear fuel reprocessing plant to reclaim residual uranium from spent, highly enriched nuclear fuels. Fuel processing as discontinued and the INTEC mission has changed. Waste left as a liquid from fuel processing and decontamination activities, is calcined into solids granules for interim storage in high integrity solid storage bins and vaults. Liquid and gaseous waste streams from these processes are treated to comply with DOE and environmental standards.

Both assessed software systems are located at INTEC. The Liquid-Gaseous Waste Distributed Control System (LGWDCS) monitors and controls High Level Waste processes. The Criticality Alarm System (CAS) detects criticality situations and emits warnings to building occupants.

The assessment team consisted of Robert Blyth with the NE-ID - Office of Technical Support, and Edward Branagan, with the DOE Headquarters - Office of Nuclear Energy, Science, Office of Integrated Safety and Project Management. More detailed biographies are available in the Biographies of Team Members section of the report.

Using an assessment plan and criteria based on the "Criteria and Guidelines for the Assessment of Safety System Software and Firmware at Defense Nuclear Facilities", the team examined objective evidence and interviewed key personnel to arrive at their conclusions regarding the reliability and robustness of the assessed software systems.

TAILORING

The assessment team saw little need to adjust the assessment criteria and guidelines contained in Criteria and Guidelines for the Assessment of Safety System Software and Firmware at Defense Nuclear Facilities.

The following changes, designated by underlined text, were implemented in this assessment.

Topical Area:

Software Requirement Description

Objective:

I&C software functions, requirements, and their bases are defined, documented and controlled

Software Configuration Management

Criteria:

All software components and products to be managed are identified and controlled.

Procedures for modifications to those components and products are followed and controlled.

Software Procurement

Criteria:

Agreements for the acquisition of software programs or components identify the functional, operational and quality requirements appropriate for their use.

ASSESSMENT RESULTS

Liquid/Gaseous Waste DCS

1. Software Requirements Description

The Liquid-Gaseous Waste Distributed Control System (LGWDCS) monitors and controls processes in the High Level Waste area of the plant The LGWDCS safety documentation and system documentation was reviewed. PSD-8.6, "Idaho Chemical Processing Plant Safety Document," Section 8.6, Management of Radioactive Airborne Effluent, describes the safety basis for the gaseous waste part of the LGWDCS.

Briefly, Section 11, Safety-Related Requirements, of Section 8.6 states that there are no structures, systems and components (SSCs) within the ventilation and off-gas systems that are engineered safety features. However, there are SSCs within the ventilation and off-gas systems that prevent or mitigate radiological releases, but the consequences of their failure are not within a safety class or engineered safety feature (ESF) realm of probability, consequence, and risk. Technical Specifications/Standards (TS 8.6B2, "Standard Main Stack (CPP-708) Radiation Monitor Operability Requirements," states that a particulate sample stream shall be continuously monitored. If this condition cannot be met, then specific actions are required. Similarly, TS 15B2, "Standard Group I Instruments-Operability," requires that certain instruments shall be operable, and provides actions to take if this condition can not be met.

PSD-4.2, "Idaho Chemical Processing Plant Safety Document," Section 4.2, Aqueous Liquid Waste Management, describes the safety basis for the liquid waste part of the LGWDCS. Briefly, Section 4.2.6, Operational Safety Requirements for PSD4.2, is mainly concerned with instrumentation to measure volumes and is primarily concerned with preventing criticality events.

SDD-13, "System Design Description, The Liquid/Gaseous Waste DCS (DCS-WN-900)," describes the LGWDCS. It lists the requirements and bases for the distributed control system. Section 3.3.5 of SDD-13 states that the specifics to process operations will normally be detailed, as needed, in the process specific SDD. The main requirements related to I&C software for the LGWDCS are in Section 3.2.6, Human Interface, and Section 3.3.6, Computer Hardware and Software. PLN-554, "Configuration Management Plan for the Liquid/Gaseous Waste Distributed Control System (LGWDCS), DCS-WN-900," (Section 3 and Appendix A) lists the safety category of the more than 20 SSCs that comprise the LGWDCS.

All of the SSCs are designated Consumer Grade (i.e., the lowest class), except for four SSCs: (1) Ventilation APS Off-gas and Process Equipment Waste (PEW) Power System overall; (2) Main Stack Power System Overall; (3) PEW Controller Rack System in PCU-WN-5, including controllers, slaves, terminations and associated local communications cabling; and (4) Main Stack Monitor Controller Rack System in PCU-OGF-6, including controllers, slaves, terminations and associated local communications cabling. The safety documentation for the LGWDCS is being revised and the main stack monitor and its power system are not expected to remain safety significant SSCs. All of the criteria are met.

2. Software Design Description

SDD-13 (Appendix D) provides the history of the LGWDCS. The system was initially installed for the Rare Gas Plant. Major upgrades have occurred and the system has evolved over the more than 15 years that it has been operating. The system is routinely calibrated and checked.

INEEL has a configuration management database that cross-references the documentation for changes to the Document Management and Control System (DMCS). Recent documents can be quickly retrieved electronically. Older documents are on microfiche and the oldest documents are in file repositories in other states. Two changes to the LGWDCS (i.e., a change to the Main Stack Monitor (CSCF-54), and a change to the Process Equipment Waste (CSCF-202)) were reviewed, and the software related requirements appeared to be appropriately implemented in the design.

MCP-3630, "I&C Computer System Management," was reviewed. The procedure is used "to manage the life-cycle process for I&C computer systems and software applications at INEEL...". It includes establishing and maintaining configuration management of computer system baselines. All of the criteria are met.

3. Software Verification and Validation

PRD-5092, "Software Quality Assurance," identifies the requirements and responsibilities for controlling the quality of computer software. Section 4.1.2 describes the requirements for verification and validation of computer software. A graded approach is allowed based on the complexity of the software, the degree of standardization, similarity with previously proved software, and importance to safety. ANS 10.4, "Guidelines for the Verification and Validation of Scientific and Engineering Computer programs for the Nuclear Industry," allows an a posteriori V&V. The a posteriori review can take advantage of program development products as well as user experience. Two changes to the software were reviewed and appropriate testing was included in the modification. All of the criteria are met.

4. Software User Documentation

Documents, such as software drawings, exist to aid users in operating the software and to assist for error conditions. The reviewer scanned examples of software drawings. The information in these drawings would assist future software modifications.

SDD-13 (Section 3.3.6, Computer Hardware and Software) describes the requirements and limitations of the system (e.g., operating system versions, minimum disk and memory requirements, and any known incompatibilities with other software).

TPR-7258, "Liquid/Gaseous Waste Bailey DCS Setting of Alarm/Switch Points," provides the procedure for setting alarm points. TPR-6948, "Bailey Network 90 Distributed Control System (DCS)," provides the procedure to take instruments out of service and to return them to service. All of the criteria are met.

5. Software Configuration Management

   PLN-554, "Configuration Management Plan for the Liquid/Gaseous Waste Distributed Control System (LGWDCS), DCS-WN-900," (Section 3 and Appendix A) identifies the configured items, their quality level and safety category. Only four items are listed as SS; all of the others are listed as Consumer Grade. System operational parameters are listed for the LGWDCS hardware and software. The software is a mixture of user-configurable and ABB designed parts. The Computer System Change Control Board (CSCCB) must approve any changes of the configured items that require a CSCF.

   MCP-3630 provides the procedures to manage modifications. Two changes to the LGWDCS (i.e., a change to the Main Stack Monitor (CSCF-54), and a change to the Process Equipment Waste (CSCF-202)) were reviewed and the documentation was appropriate. No discrepancies were noted in following MCP-3630. All of the criteria are met.

6. Software Quality Assurance

   PRD-5092, "Software Quality Assurance," identifies the requirements and responsibilities for controlling the quality of computer software. PDD-122, "Software Quality Assurance Program," states, " the software quality assurance program covers all company software application (see def.) activities and operations at INEEL." It includes figures that depict the basis, requirements and implementation of the SQA requirements, and the related procedures. All of the criteria are met.

7. Software Procurement

   Not applicable.

8. Software Problem Reporting and Corrective Action

   MCP-598 provides the procedure for INEEL to report, track, and resolve problems or issues for systems such as the LGWDCS. Responsibilities are also described in MCP-598. All of the criteria are met.

In conclusion, all of the criteria were met. No issues were identified for the LGWDCS.

Criticality Alarm System CAS

The CAS is considered a legacy system. Applicable INEEL software Quality Assurance procedures and PLN-1326, "Criticality Alarm System Computer Software Configuration Management Plan" currently controls the software. Further software upgrades are unlikely.

"The CAS system is approaching the end of its life cycle. Two scenarios need to be considered. One alternative is the system design will have to be upgraded to compensate for replacement parts no longer available for maintenance. The other and preferred alternative is to obtain a replacement device before the present systems fail. Use a Form 562.15, "Computer System Change Form," (CSCF; see def.) or Form 431.37, "Engineering Change Form," (ECF) to retire the equipment, per MCP-3630."[1]

The assessment team concludes that review criteria established by DOE in its implementation of "Implementation Plan (IP) for DNFSB Recommendation 2002-1," is met.

The assessment team identified no concerns or findings.

A System Description Document is currently being generated. PLN-1326 was issued two weeks before the start of the assessment field investigation. A brief follow assessment to verify completion of the System Description Document and implementation of PLN-1326 is recommended.

[1] PLN-1326, Criticality Alarm System Computer Software Configuration Management Plan, Section 2.1 CAS retirement Policy

LESSONS LEARNED

The following best practice extends lessons learned by NE-ID in assessment QSD 2004-62.

The assessment team copied the assessment criteria from Criteria and Guidelines for the Assessment of Safety System Software and Firmware at Defense Nuclear Facilities and inserted the criteria directly into a conventional audit checklist format. These checklists were then emailed to the assessed organization. The assessed organization inserted URL's in the check lists, to documents in the site Electronic Document Management system, that furnished objective evidence that the associated criteria was met. The modified checklists were then emailed to assessment team members. This enabled the assessment team to work remotely and saved the assessed organization time normally spent retrieving and copying documentation requested by the assessment team.

Both the assessing and assessed organizations believe that this methodology reduced the amount of time they spent in the assessment by roughly 25%, over conventional methodologies.

A more detailed description of this methodology is available on the DOE-EH-SQA web site under lessons learned (http://www.eh.doe.gov/sqa/lessons_learned.htm).

DETAILED RESULTS

Liquid/Gaseous Waste Distributed Control System

See Appendix A for detailed results of the Liquid/Gaseous Waste Distributed Control System.

Criticality Alarm System

See Appendix B for detailed results of the Criticality Alarm System

DOCUMENTS AND REFERENCES

Criteria and Guidelines For the Assessment of Safety System Software and Firmware at Defense Nuclear Facilities, CRAD - 4.2.3.1 Revision 3, October 24, 2003

ANS 10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer programs for the Nuclear Industry," 1987.

CSCF-54, "Change to the Main Stack Monitor," March 2000.

CSCF-202, "Change to the Process Equipment Waste," September 2002.

EAR-156, "LET&D- Total Loss of DCS," Rev. 0, September 2003.

EAR-177, "PEW Total Loss of DCS," Rev. 0, September 2003.

EAR-178, "PEW Temperature Instrument Alarm or Failure," Rev. 1, December 2003.

MCP-123, "Unreviewed Safety Questions," Rev. 7, August 2002.

MCP-540, "Documenting the Safety Category of Structures, Systems, and Components," Rev. 13, March 2001.

MCP-598, "Corrective Action System," Rev. 16, September 2003.

MCP-3630, "I&C Computer System Management," Rev. 4, July 2003.

PDD-122, "Software Quality Assurance Program," Rev. 0, July 2003.

PLN-554, "Configuration Management Plan for the Liquid/Gaseous Waste Distributed Control System (LGWDCS), DCS-WN-900," Rev. 1, February 2003.

PRD-5092, "Software Quality Assurance," Rev. 4, November 2002.

PSD-4.2, "Idaho Chemical Processing Plant Safety Document," Section 4.2, "Aqueous Liquid Waste Management," Rev. 11, February 2002.

PSD-8.6, "Idaho Chemical Processing Plant Safety Document," Section 8.6, "Management of Radioactive Airborne Effluent," Rev. 0a, November 2000.

Safety Category List, "Liquid/Gaseous Waste DCS (DCS-WN-900)," August 2002.

SDD-13, "System Design Description, The Liquid/Gaseous Waste DCS (DCS-WN-900)," Rev. 0, November 2000.

TPR-7258, "Liquid/Gaseous Waste Bailey DCS Setting of Alarm/Switch Points," Rev. 0, September 2003.

TPR-6948, "Bailey Network 90 Distributed Control System (DCS)," Rev. 0, September 2003.

Work Order 002033101, "Upgrade WPCS Computer Interface," October 2000.

PEOPLE CONTACTED

Name	Title	Email address
C.G. Rieger	ADVISORY ENGR/SCI	CRIEGER@inel.gov
S. E. Holaday	ADVISORY ENGR/SCI	SHOLADAY@inel.gov
E. Klingler	STAFF ENGINEER/SCIENTIST	ERK@inel.gov

SOFTWARE QUALITY ASSURANCE DATA

Not applicable

BIOGRAPHIES OF TEAM MEMBERS

Bob Blyth is the NE-ID designated subject matter expert for software quality assurance. He has certifications as a Professional Engineer, Quality Manager, Professional Mediator and Leader Auditor. He is currently the Program Manager for the National Spent Nuclear Fuel program Quality Assurance Program. In the last 5 years he has lead 5 major QA audits of DOE facilities and participated as an auditor in 12 other major QA DOE program audits.

Ed Branagan is a nuclear engineer with the Office of Nuclear Energy, Science & Technology/Office of Integrated Safety and Project Management (NE-70). He is certified by the American Board of Health Physics, and has a BA in Physics, and a Ph.D. in Radiation Biophysics. He currently serves as the Office of Nuclear Energy Science and Technology's contact on radiation protection and quality assurance issues. His work has involved: performing accident analyses and health physics assessments; directing reviews of Environmental Impact Statements, Self-Assessments, Safety Analysis Reports, and Technical Safety Requirements; and conducting Operational Readiness Reviews. Prior to joining DOE, he was a senior health physicist with the Nuclear Regulatory Commission (NRC, 1976-1988).

APPENDIX A

Detailed assessment results of the Liquid-Gaseous Waste Distributed Control System Software

1. Prepared by: R. L. Blyth	2. Date Prepared: 4/9/2004	3. Type of Checklist:	Software, DNFSB X External ☐ Internal
4. Organization / System Evaluated: INEEL / BBWI/ INTEC Liquid / Gaseous Waste DCS Identifier 113755	5. Evaluation Dates: 4/26/ to 4/30/2004	6. Source/Requirements Document: DNFSB Recommendation 2002-1 Implementation Plan CRAD - 4.2.3.1, Rev 3	

7. Checklist Completed by:

Assessor:	Edward F. Branagan, Jr.	/s/	5/26/2004
	Print/Type Name	Signature	Date

8. Personnel Contacted:

Topical Area: 1. Software Requirement Description	Objective: I&C software functions, requirements, and their bases are defined, documented and controlled.
Criteria	Comments/Notes/ Results
1. The functional and performance requirements for the I&C software are complete, correct, consistent, clear, testable, and feasible.	Example CSCF-54: http://xena/edm00l/3735/933588.tif LGWDCS SDD-13: http://xena/edm00j/3607/901560.tif SDD-13, "System Design Description, The Liquid/Gaseous Waste DCS (DCS-WN-900)" describes the LGWDCS. SDD-13 lists the requirements and bases for the distributed control system (DCS). Specifics to process operations are normally covered, as needed, by a process SDD. The safety documentation for the LGWDCS is being revised, and it is not expected that the main stack monitor will continue to be a safety significant SSC. The main requirements related to I&C software for the LGWDCS are in Section 3.2.6, Human Interface, and Section 3.3.6, Computer Hardware and Software. Functional requirements are contained in Plant Safety Documents (i.e., PSD-4.2 and PSD-8.6). Criteria 1 is met.

2.	The I&C software requirements are documented and consistent with the system safety basis.	There were no safety basis requirements affected by this CSCF. The USQ process would confirm this per MCP-123 and the PSD applicable to the process system is PSD-8.6. MCP-123: http://xena/edm02e/6303/1575641.tif PSD-8.6: http://xena/edm03d/7040/1759980.tif The current process for safety basis implementation is covered under MCP-1135. All TS/S for this system were implemented and use governed by operating procedures before MCP-1135 was put in place. EAR-178 is an example of a operating procedure that refers to a TS/S instrument on the DCS . MCP-1135: http://xena/edm03l/9967/2491574.tif EAR-178: http://xena/edm03l/9974/2493486.tif The safety basis for radioactive airborne effluents is contained in PSD-8.6, in particular, see Section 11, Safety Related Requirements. PSD-4.2, Idaho Chemical Processing Plant Safety Document, Section 4.2, Aqueous Liquid Waste Management, describes the safety basis for liquid waste management. Section 4.2.6, Operational Safety Requirements for PSD4.2, is mainly concerned with instrumentation to measure volumes and preventing criticality events. Criteria 2 is met.
3.	The software requirements description (SRD) is controlled and maintained.	SDD-13 is controlled and maintained. Criteria 3 is met.
4.	Each requirement should be uniquely identified and defined such that it can be objectively verified and validated.	MCP-3630 (e.g., see Section 4.5 and Appendix F) indicates that the technical and functional requirements of major changes to I&C computer systems must be idenfitied. SDD-13 (e.g., page 21, Section 4.1) states that the consoles (which contain software) are uniquely identified. Criteria 4 is met.

Software Requirement Description
Approach:

Review the appropriate safety basis documents, such as DSAs, SARs, TSRs, and system documentation such as the system design description, and procurement specifications, to determine if the I&C software requirements are consistent with the safety system design and safety basis. These requirements may exist either as a standalone document (e.g., SRD) or embedded in another. Determine if the following types of requirements are addressed as appropriate:

- Functionality - the safety functions the software is to perform during normal, abnormal, and emergency situation;
- Performance - precision and accuracy requirements and the time-related issues of software operation such as time-dependent input-to-output relations, speed, recovery time, response time, frequency of reading input and updating output, throughput, and interrupt handling;
- Design constraints - any elements that will restrict design options;
- Attributes - non-time-related issues of software operation such as portability, acceptance criteria, security, access control, and maintainability; and
- External interfaces - interactions with people, hardware, and other software.

Determine whether the documents containing the software requirement description are controlled under configuration change control and document control processes. Verify these documents are reviewed and updated as necessary.
If the above requirements are not available in system or software level documentation, the perceived software requirements may be identified through available documentation and discussions with the program developer, users, and sponsor. These perceived requirements will then be used as the basis for other topical area assessment activities.

Discussion
The Liquid-Gaseous Waste Distributed Control System (LGWDCS) monitors and controls processes in the High Level Waste area of the plant. The LGWDCS safety documentation and system documentation was reviewed. PSD-8.6, "Idaho Chemical Processing Plant Safety Document," Section 8.6, Management of Radioactive Airborne Effluent, describes the safety basis for the gaseous waste part of the LGWDCS.
Briefly, Section 11, Safety-Related Requirements, of Section 8.6 states that there are no structures, systems and components (SSCs) within the ventilation and off-gas systems that are engineered safety features. However, there are SSCs within the ventilation and off-gas systems that prevent or mitigate radiological releases, but the consequences of their failure are not within a safety class or engineered safety feature (ESF) realm of probability, consequence, and risk. Technical Specifications/Standards (TS 8.6B2, "Standard Main Stack (CPP-708) Radiation Monitor Operability Requirements," states that a particulate sample stream shall be continuously monitored. If this condition cannot be met, then specific actions are required. Similarly, TS 15B2, "Standard Group I Instruments-Operability," requires that certain instruments shall be operable, and provides actions to take if this condition cannot be met.
PSD-4.2, "Idaho Chemical Processing Plant Safety Document," Section 4.2, Aqueous Liquid Waste Management, describes the safety basis for the liquid waste part of the LGWDCS. Briefly, Section 4.2.6, Operational Safety Requirements for PSD4.2, is mainly concerned with instrumentation to measure volumes and is primarily concerned with preventing criticality events.
SDD-13, "System Design Description, The Liquid/Gaseous Waste DCS (DCS-WN-900)," describes the LGWDCS. It lists the requirements and bases for the distributed control system. Section 3.3.5 of SDD-13 states that the specifics to process operations will normally be detailed, as needed, in the process specific SDD. The main requirements related to I&C software for the LGWDCS are in Section 3.2.6, Human Interface, and Section 3.3.6, Computer Hardware and Software. PLN-554, "Configuration Management Plan for the Liquid/Gaseous Waste Distributed Control System (LGWDCS), DCS-WN-900," (Section 3 and Appendix A) lists the safety category of the more than 20 SSCs that comprise the LGWDCS.
All of the SSCs are designated Consumer Grade (i.e., the lowest class), except for four SSCs: (1) Ventilation APS Off-gas and Process Equipment Waste (PEW) Power System overall; (2) Main Stack Power System Overall; (3) PEW Controller Rack System in PCU-WN-5, including controllers, slaves, terminations and associated local communications cabling; and (4) Main Stack Monitor Controller Rack System in PCU-OGF-6, including controllers, slaves, terminations and associated local communications cabling. The safety documentation for the LGWDCS is being revised and the main stack monitor and its power system are not expected to remain safety significant SSCs. All of the criteria are met.

Topical Area: 2. Software Design Description	Objective: The software design description (SDD) depicting the logical structure, information flow, logical processing steps, and data structures are defined and documented.
Criteria	Comments/Notes/ Results
1. All I&C software related requirements are implemented in the design.	Example CSCF-54: http://xena/edm00l/3735/933588.tif SD-13 (Appendix D) provides the history of the LGWDCS. The system was initially installed for the Rare Gas Plant. Major upgrades have occurred and the system has evolved over the more than 15 years that it has been operating. The system is routinely calibrated and checked. INEEL has a configuration management database that cross-references the documentation for changes to the Document Management and Control System (DMCS). Recent documents can be quickly retrieved electronically. Older documents are on microfiche and the oldest documents are in file repositories in other states. Two changes to the LGWDCS (i.e., a change to the Main Stack Monitor (CSCF-54), and a change to the Process Equipment Waste (CSCF-202)) were reviewed, and the software related requirements appeared to be appropriately implemented in the design. Criteria1 is met.
2. All design elements are traceable to the requirements.	The design development process, expectations and reviews are covered by MCP-3630. MCP-3630 http://xena/edm03g/9483/2370553.tif MCP-3630, "I&C Computer System Management," was reviewed. The procedure is used "to manage the life-cycle process for I&C computer systems and software applications at INEEL..." It includes establishing and maintaining configuration management of computer system baselines. Criteria 2 is met.
3. The design is correct, consistent, clearly presented, and feasible.	The design development process, expectations and reviews are covered by MCP-3630. MCP-3630 http://xena/edm03g/9483/2370553.tif Criteria 3 is met. See preceeding.

Software Design Description
Approach:

Review the appropriate documents, such as vendor specifications for I&C software design, description of the components and subcomponents of the software design, including databases and internal interfaces. The design may be documented in a standalone document such as an SDD or embedded in other documents. The SDD should contain the information listed below:

- A description of the major safety components of the software design as they relate to the I&C software requirements and any interactions with non-safety components.
- A technical description of the software with respect to control flow, control logic, mathematical model, and data structure and integrity.
- A description of the allowable or prescribed ranges for inputs and outputs.
- A description of error handling strategy and use of interrupt protocols.
- The design described in a manner suitable for translating into computer codes.

Note: In instances where software design documentation is not available, the contractor may be able to construct a design summary on the basis of available program documentation, review of the source code (if applicable), and information from the facility staff. Care should be taken to ensure that such a design summary is consistent with the complexity and importance of the software to the safety functions.

Discussion
See comments for individual criteria.

Topical Area: 3. Software Verification and Validation	Objective: The V&V process and related documentation for I&C software are defined and maintained to: ensure that the software adequately and correctly performs all its intended functions; ensure that the software does not perform any adverse unintended function.
Criteria	Comments/Notes/ Results
1. All I&C software requirements and design have been verified and validated for correct operation using testing, observation or inspection techniques.	MCP-3630 covers design review requirements and expectations. MCP-3630 http://xena/edm03g/9483/2370553.tif An example of a change to the LGWDCS is in contained in CSCF-54: http://xena/edm00l/3735/933588.tif PRD-5092, Software Quality Assurance, identifies the requirements and responsibilities for controlling the quality of computer software. Section 4.1.2 describes the requirements for verification and validation of computer software. A graded approach is allowed based on the complexity of the software, the degree of standardization, similarity with previously proved software, and importance to safety. ANS 10.4, "Guidelines for the Verification and Validation of Scientific and Engineering Computer programs for the Nuclear Industry," allows an a posteriori V&V. The a posteriori review can take advantage of program development products as well as user experience. Two changes to the software were reviewed and appropriate testing was included in the modification. Criteria 1 is met.
2. Relevant abnormal conditions have been evaluated for mitigating unintended functions through testing, observation or inspection techniques.	Relevant abnormal conditions were considered in the development of the test included with the CSCF-54. Criteria 2 is met.

Software Verification and Validation
Approach:

Review appropriate documents, such as test plans, test cases, test reports, system qualification plans and reports, and vendor qualification reports to determine if:

- An established process for validating the requirements exists.
- The V&V process includes an assessment to demonstrate whether the software requirements and system requirements are correct, complete, accurate, consistent, and testable.
- Dynamic testing has been performed to confirm time-dependent input-output relations, speed, recovery time, response time, frequency of reading input and updating output, throughput, and interrupt handling, as specified in the SRD.
- Each test case is executed in accordance with the test procedures and test plan.
- Correct inputs have been used for each test case.
- Sufficient number of tests has been executed to test all I&C software requirements.
- Tests representative of the anticipated application have been executed.
- Hardware and software configurations pertaining to the software V&V are specified.
- Results of V&V activities including test execution, observations, inspections and reviews are documented.
- V&V is complete and all unintended conditions are dispositioned before software is approved for use.
- Traceability exists from software requirements to design and testing, and, as appropriate, to user documentation.
- V&V is performed by individuals or organizations that have sufficient independence from the creation of I&C software.
- For SSCs that have been in operation for several years, the team should consider using an approach similar to an ANS 10.4 *a posteriori* review.

Discussion
See comments for individual criteria.

Topical Area: 4. Software User Documentation	Objective: Software documentation is available to guide the user in installing, operating, managing, and maintaining the I&C software.
Criteria	Comments/Notes/ Results
1. The system requirements and constraints, installation procedures, and maintenance procedures such as database fine-tuning are clearly and accurately documented.	Example CSCF-54: http://xena/edm00l/3735/933588.tif LWGDCS PLN-554: http://xena/edm03a/6866/1716310.tif System Layout Drawing: http://xena/edm02/a184/a45126.tif Example Loop Drawings: http://xena/edm02/a152/a37542.tif http://xena/edm02/a153/a37577.tif Example Software Drawings: http://hlwo.inel.gov/dcs/bin/CAD_Browse.pl/CAD_Frame/6_2/1060211 http://hlwo.inel.gov/dcs/bin/CAD_Browse.pl/CAD_Frame/6_2/1060209 Example DCS Procedures: http://xena/edm03i/9686/2421392.tif http://xena/edm03i/9712/2427910.tif Example Operations Procedures: http://xena/edm03i/9667/2416572.tif http://xena/edm03i/9665/2416157.tif System Vendor Documentation: http://hlwo.inel.gov/dcs/bin/DCS_Manuals.pl Additional installation instructions, beyond the guidance given in PLN-554, are provided in work planning packages or test procedures. An example of a work-planning package to install some hardware is below. Example WO: http://xena/edm02b/5936/1483779.tif PLN-554, "Configuration Management Plan for the Liquid/Gaseous Waste Distributed Control System (LGWDCS), DCS-WN-900," (Section 3 and Appendix A) specifically identifies the configured items, their quality level and safety category. Only four items are listed as SS; all of the others are listed as Consumer Grade. System operational parameters are listed for the LGWDCS hardware and software. The software is a mixture of user-configurable and ABB designed parts. The Computer System Change Control Board (CSCCB) must approve any changes of the configured items that require a CSCF. Craig Rieger is identified as the cognizant engineer for the CSCCB on the LGWDCS. TPR-7258, Liquid/Gaseous Waste Bailey DCS Setting of Alarm/Switch Points, provides the procedure for setting alarm points. TPR-6948, Bailey Network 90 Distributed Control System (DCS)," provides the procedure to take instruments out of service and to return them to service. Examples of software drawings (e.g., Reference Drawing # 095353) were reviewed. This criteria is met.
2. Any operational data system requirements and limitations are clearly and accurately documented.	PLN-554 lists the operational parameters. Criteria 2 is met.

3.	Documentation exists to aid the users in the correct operation of the software and to provide assistance for error conditions.	Documents, such as software drawings, exist to aid users in operating the software and to assist for error conditions. The reviewer scanned examples of software drawings. The information in these drawings would assist future software modifications. Criteria 3 is met.
4.	Appropriate software design and coding documentation to assist in any future software modifications is defined and documented.	SDD-13 (Secton 3.3.6, Computer Hardware and Software) describes the requirements and limitations of the system (e.g., operating system versions, minimum disk and memory requirements, and any known incompatibilities with other software). Criteria 4 is met.

Software User Documentation
Approach:

The team will review the user's manual and related documents. These documents may exist either as a standalone documents or embedded in other documents. The user documentation should contain:

- User instructions that contain an introduction, a description of the user's interaction with the software, and a description of any required training necessary to use the software.
- Input and output specifications appropriate for the function being performed.
- A description of user messages or other indications as a result of improper input or system problems, and user response.
- Information for obtaining user and maintenance support.
- A description of system requirements and limitations such as operating system versions, minimum disk and memory requirements, and any known incompatibilities with other software.
- A description of any system requirements or limitations for operational data such as file sizes.
- Recommendations for routine database maintenance and instructions for performing this maintenance.
- Design diagrams, structure or flow charts, pseudo code, and source code listings necessary for performing future modifications of custom software.

Discussion
See comments for individual criteria.

Topical Area: 5. Software Configuration Management		Objective: Software components and products are identified, managed, and changes to those items are controlled.
Criteria		Comments/Notes/ Results
1.	All software components and products to be managed are identified and controled.	LWGDCS PLN-554: http://xena/edm03a/6866/1716310.tif MCP-3630 http://xena/edm03g/9483/2370553.tif Safety Categorization Forms: http://xena/edm03a/6796/1698826.tif http://xena/edm03a/6796/1698828.tif PLN-554 (e.g., see Section 3 and Appendix A) identifies the components of the LWGDCS that are controlled. Section 11 of PLN-554 describes the process for status tracking and control of baselines. MCP-3630 provides the procedures to manage the modifications. Criteria 1 and 2 for this topical area are met. Two changes to the LGWDCS (i.e., a change to the Main Stack Monitor (CSCF-54), and a change to the Process Equipment Waste (CSCF-202)) were reviewed and the documentation was appropriate. For example, TFR-21, Auto-Suppression of Ration Indications for Offline Main Stack Train (T&FR for CSCR-54) follows the format of Appendix F of MCP-3630. CSCF-54 involved an enhancement requested by Operations to remove a nuisance alarm situation.
2.	For those components and products procedures exist to manage the modification and installation of new versions.	See references under item 1.
3.	Procedures for modifications to those components and products are followed and controled.	Example CSCF-54: http://xena/edm001/3735/933588.tif System Log Examples http://hlwo.inel.gov/dcs/bin/MyDBD.pl?Table=ci&What=Search http://hlwo.inel.gov/dcs/bin/MyDBD.pl?Table=cse&What=Search http://hlwo.inel.gov/dcs/bin/MyDBD.pl?Table=failure&What=Search CSCF-54 and CSCF-202 were reviewed and no discrepancies in following procedures were noted.

Software Configuration Management
Approach:

Review appropriate documents such as applicable procedures related to I&C software change control to determine if a software configuration management process exists and is effective. This determination is made based on the following actions.

- Verify the existence of a software configuration management plan, either in standalone form or embedded in another document.
- Verify that a configuration baseline is defined and that it is being adequately controlled. This baseline should include operating system components, any associated runtime libraries, acquired software executables, custom-developed source code files, users' documentation, the appropriate documents containing software requirements, software design, software V&V procedures, test plans and procedures, and any software development and quality planning documents.
- Review procedures governing change management for installation of new versions of the software components including new releases of acquired software.
- Review software change packages and work packages to ensure that:
  possible impacts of software modifications are evaluated before changes are made,
  various software system products are examined for consistency after changes are made,
  software is tested according to established standards after changes have been made.
- Verify by sampling that documentation affected by software changes accurately reflects all safety-related changes that have been made to the software.
- Interview a sample of cognizant line, engineering, Quality Assurance (QA) managers, and other personnel to verify their understanding of the change control process and commitment to manage changes affecting design, safety basis, and software changes in a formal, disciplined, and auditable manner.

Discussion
PLN-554, "Configuration Management Plan for the Liquid/Gaseous Waste Distributed Control System (LGWDCS), DCS-WN-900," (Section 3 and Appendix A) identifies the configured items, their quality level and safety category. Only four items are listed as SS; all of the others are listed as Consumer Grade. System operational parameters are listed for the LGWDCS hardware and software. The software is a mixture of user-configurable and ABB designed parts. The Computer System Change Control Board (CSCCB) must approve any changes of the configured items that require a CSCF.

MCP-3630 provides the procedures to manage modifications. Two changes to the LGWDCS (i.e., a change to the Main Stack Monitor (CSCF-54), and a change to the Process Equipment Waste (CSCF-202)) were reviewed and the documentation was appropriate. No discrepancies were noted in following MCP-3630. All of the criteria are met.

Topical Area: 6. Software Quality Assurance		Objective: Software quality activities are evaluated for applicability to the I&C software, defined to the appropriate level of rigor, and implemented.
Criteria		Comments/Notes/ Results
1.	Software quality activities and software practices for requirements management, software design, software configuration management, procurement controls, verification and validation including reviews and testing, and documentation have been evaluated and established at the appropriate level for proper applicability to the I&C software under assessment.	PRD-5092, Software Quality Assurance, identifies the requirements and responsibilities for controlling the quality of computer software. PDD-122, Software Quality Assurance Program, states, "the software quality assurance program covers all company software application (see def.) activities and operations at INEEL." It includes figures that depict the basis, requirements and implementation of the SQA requirements, and the related procedures. MCP-3630, "I&C Computer System Management," provides the procedures to establish and maintain computer system baselines for I&C computer systems. This is a relatively new procedure (July 2003). Based on the preceding and the review of two specific changes to the LGWDCS, criteria 1 and 2 are met.
2.	The software quality activities have been effectively implemented.	This criteria is met. See preceding.

Software Quality Assurance
Approach:

The team will confirm the existence of an SQA Plan, either as a standalone document or embedded in another document, and related procedures, QA assessment reports, test reports, problem reports, corrective actions, supplier control, and training, and determine the effectiveness of the SQA program. The assessment also entails interviewing managers, engineers, operators, and software users. The SQA Plan shall identify:

- The software products to which the Plan applies.
- The organizations responsible for maintaining software quality, along with their tasks and responsibilities.
- Required documentation such as SRD, SDD, V&V, SCM, and software user documentation.
- Supplier control provisions for meeting established requirements.
- Standards, conventions, techniques, or methodologies that guide software development and ensure compliance to the same.
- Methods for error reporting and corrective action.

Any tailoring or note of non-applicability of software quality activities.
Through the assessment of other topical areas, the effectiveness of implementing the software quality activities will be noted.

Discussion

PRD-5092, "Software Quality Assurance," identifies the requirements and responsibilities for controlling the quality of computer software. PDD-122, "Software Quality Assurance Program," states, "the software quality assurance program covers all company software application (see def.) activities and operations at INEEL." It includes figures that depict the basis, requirements and implementation of the SQA requirements, and the related procedures. All of the criteria are met.

Topical Area: 7. Software Procurement	Objective: Acquired software meets the applicable level of software quality to ensure the safe operation of the system.
Criteria	Comments/Notes/ Results
1. Agreements for the acquisition of software programs or components identify the functional, operational and quality requirements appropriate for their use.	Not applicable.
2. Acquired software is verified to meet the identified quality requirements.	Not applicable.

Software Procurement
Approach:

Vendors that supply COTS and other types of acquired software are evaluated to ensure that the software is developed under an appropriate quality assurance program and are capable of providing software that satisfies the specific requirements. The volume of commercial use for the vendor software, especially with COTS software, should be considered in determining the adequacy of the vendor's quality assurance program. The assessment of software procurements shall include the following:

Determine the existence of acquired software quality requirements. These requirements may be embedded in the DOE contractors' or subcontractors' procurement requirements or processes, software or system requirements description, software or system design description, or a software quality plan.

Review the methods used to verify that acquired software meets the specified quality requirements, and determine if these methods accomplish those requirements. These methods may be included in a software quality plan or software test plan.

Review evidence that the acquired software was evaluated for the appropriate level of quality. This evidence may be included in test results, a test summary, vendor site visit reports, or vendor quality program assessment reports.

Topical Area: 8. Software Problem Reporting and Corrective Action	Objective: A process for I&C software problem reporting is established, maintained, and controlled, including notification of errors, failures, and corrective action development.
Criteria	Comments/Notes/ Results
1. Documented practices and procedures for reporting, tracking, and resolving problems or issues are defined and implemented.	LWGDCS PLN-554: http://xena/edm03a/6866/1716310.tif MCP-3630 http://xena/edm03g/9483/2370553.tif MCP-598 http://xena/edm03i/9756/2438962.tif Note: CSCF-54 is an example of an operator observation, in this case a nuisance alarm, whose response was a modification under a CSCF. Also see link to failure log below. Example CSCF-54: http://xena/edm00l/3735/933588.tif DCS failure log: http://hlwo.inel.gov/dcs/bin/MyDBD.pl?Table=failure&What=Search MCP-598 provides the procedure for INEEL to report, track, and resolve problems or issues for systems such as the LWGDCS. Responsibilities are also described in MCP-598. Criteria 1 and 2 are met.
2. Organizational responsibilities for reporting issues, approving changes and performing corrective actions are identified and effective.	LWGDCS PLN-554: http://xena/edm03a/6866/1716310.tif MCP-3630 http://xena/edm03g/9483/2370553.tif Criteria 2 is met. See preceding.

Software Problem Reporting and Corrective Action
Approach:

Review documents and interview facility staff for the problem reporting and notification process to determine if:

- A formal procedure exists for software problem reporting and corrective action development that addresses software errors, failures, and resolutions.
- The problems that impact the operation of the software are promptly reported to affected organizations.
- Corrections and changes are evaluated for impact and approved prior to being implemented.
- Corrections and changes are verified for correct operation and to ensure no side effects were introduced.
- Preventive measures and corrective actions are provided to affected organization in a timely manner associated with the impact of the original defect.
- The organizations responsible for problem reporting and resolution are defined.

Discussion
See comments for individual criteria.

APPENDIX B

Detailed Assessment Results of the Criticality Alarm System Software

1. Prepared by: R.L. Blyth	2. Date Prepared: 4/9/2004	3. Type of Checklist:	Software, DNFSB X External ☐ Internal
4. Organization / System Evaluated: INEEL / BBWI/ INTEC Identifier 113755 Criticality Alarm System	5. Evaluation Dates: 4/26/ to 4/30/2004	6. Source/Requirements Document: DNFSB Recommendation 2002-1 Implementation Plan CRAD - 4.2.3.1, Rev 3	

7. Checklist Completed by:

Assessor: R.L. Blyth (Print/Type Name) /s/ (Signature) 5/26/2004 (Date)

8. Personnel Contacted: C.G. Rieger, E. Klingler, S. Holladay

Topical Area: 1. Software Requirement Description	Objective: I&C software functions, requirements, and their bases are defined, documented and controlled.
Criteria	Comments/Notes/ Results
1. The functional and performance requirements for the I&C software are complete, correct, consistent, clear, testable, and feasible. PSD 4.8, http://xena/edm02h/6658/1664340.tif PSD 4.12, http://xena/edm03k/9887/2471694.tif TS 4.8B4, http://xena/edm00/3106/776258.tif TS 4.12B3, http://xena/edm02a/a252/a62094.tif TS 15B8, http://xena/edm03d/7094/1773254.tif	Criteria Met CPP 651 Failed detector and provisions for inconsistent readings among detectors are described in TS 4.8B4 Limiting Conditions for Operation are described in TS 15B8. Threshold values are documented in W.O. 5817, attachment 1, section 3.2, Check Alarm and Set Points and Background Values. CPP 603 Failed detector and provisions for inconsistent readings among detectors are described in TS 4.12B3 Limiting Conditions for Operation are described in TS 15B8. Threshold values are documented in W.O. 5818, attachment 1, section 3.2, Check Alarm and Set Points and Background Values.

2.	The I&C software requirements are documented and consistent with the system safety basis. PSD 4.8, http://xena/edm02h/6658/1664340.tif PSD 4.12, http://xena/edm03k/9887/2471694.tif TS 4.8B4, http://xena/edm00/3106/776258.tif TS 4.12B3, http://xena/edm02a/a252/a62094.tif TS 15B8, http://xena/edm03d/7094/1773254.tif	Criteria met CPP 651 PSD 4.8 Plant Safety Document Section 4.8 "Unirradiated Fuel Storage Facility" is the current documented safety analysis for the Unirradiated Fuel Storage Facility, CPP-651. Failed detector and provisions for inconsistent readings among detectors are described in TS 4.8B4 Limiting Conditions for Operation are described in TS 15B8. Implemented threshold values, documented in W.O. 5817, attachment 1, section 3.2, Check Alarm and Set Points and Background Values. Safety basis requirements from PSD 4.8 are included in various CAS software requirements document. A System Design Description is being developed that will include the safety basis requirements for the CAS and other requirements in one document. CPP 603 PSD 4.12 Plant Safety Document "Irradiated Fuel Storage Facility" is the current documented safety analysis for the Unirradiated Fuel Storage Facility, CPP-603. Failed detector and provisions for inconsistent readings among detectors are described in TS 4.12B3 Limiting Conditions for Operation are described in TS 15B8. Implemented threshold values are documented in W.O. 5818, attachment 1, section 3.2, Check Alarm and Set Points and Background Values. Safety basis requirements from PSD 4.12 are included in various CAS software requirements document. A System Design Description is being developed that will include the safety basis requirements for the CAS and other requirements in one document A Follow up assessment to verify issuing System Design Description and implementation of PLN-1326 is recommended.

3. The software requirements description (SRD) is controlled and maintained. PLN-1326, http://xena/edm04h/10369/2592131.tif	Criteria is met There is currently no software requirements description document. All the documents that contain the software requirements are controlled using the INEEL's Electronic Document Management System. System Design Descriptions for both CPP 651 and CPP-603 are currently being developed. Both will be controlled using the INEEL's Electronic Document Management System. PLN-1326, Criticality Alarm System Computer Software Configuration Management Plan describes how the configuration of the CAS systems in CPP-651 and CPP-603 will be managed. It was issued on 4/21/2004. There is not sufficient operating history or documentation to verify its implementation. Inadequate documentation of changes to CAS software was identified in ICARE Issue # 28729. Implementation of PLN-1326 should correct this. A Follow up assessment to verify issuing System Design Description and implementation of PLN-1326 is recommended.
4. Each requirement should be uniquely identified and defined such that it can be objectively verified and validated.	Criteria is met Software requirements are uniquely defined and can be identified, though they are currently found in multiple documents. Revised Safety Analysis Reports and System Design Descriptions are currently being written, which will simplify software requirements trace ability.

Software Requirement Description
Approach:

Review the appropriate safety basis documents, such as DSAs, SARs, TSRs, and system documentation such as the system design description, and procurement specifications, to determine if the I&C software requirements are consistent with the safety system design and safety basis. These requirements may exist either as a standalone document (e.g., SRD) or embedded in another. Determine if the following types of requirements are addressed as appropriate:

- Functionality - the safety functions the software is to perform during normal, abnormal, and emergency situation;
- Performance - precision and accuracy requirements and the time-related issues of software operation such as time-dependent input-to-output relations, speed, recovery time, response time, frequency of reading input and updating output, throughput, and interrupt handling;
- Design constraints - any elements that will restrict design options;
- Attributes - non-time-related issues of software operation such as portability, acceptance criteria, security, access control, and maintainability; and
- External interfaces - interactions with people, hardware, and other software.

Determine whether the documents containing the software requirement description are controlled under configuration change control and document control processes. Verify these documents are reviewed and updated as necessary.

If the above requirements are not available in system or software level documentation, the perceived software requirements may be identified through available documentation and discussions with the program developer, users, and sponsor. These perceived requirements will then be used as the basis for other topical area assessment activities.

Topical Area: 2. Software Design Description	Objective: The software design description (SDD) depicting the logical structure, information flow, logical processing steps, and data structures are defined and documented.
Criteria	Comments/Notes/ Results
1. All I&C software related requirements are implemented in the design.	Criteria is met CPP 651 PSD 4.8 Plant Safety Document Section 4.8 "Unirradiated Fuel Storage Facility" is the current documented safety analysis for the Unirradiated Fuel Storage Facility, CPP-651. Failed detector and provisions for inconsistent readings among detectors are described in TS 4.8B4 Limiting Conditions for Operation are described in TS 15B8. Implemented threshold values are documented in W.O. 5817, , attachment 1, section 3.2, Check Alarm and Set Points and Background Values. Safety basis requirements from PSD 4.8 are included in various CAS software requirements document. CPP 603 PSD 4.12 Plant Safety Document "Irradiated Fuel Storage Facility" is the current documented safety analysis for the Unirradiated Fuel Storage Facility, CPP-603. Failed detector and provisions for inconsistent readings among detectors are described in TS 4.12B3 Limiting Conditions for Operation are described in TS 15B8. Implemented threshold values, documented in W.O. 5818, attachment 1, section 3.2, Check Alarm and Set Points and Background Values. Safety basis requirements from PSD 4.12 are included in various CAS software requirements document.

2. All design elements are traceable to the requirements.	Applicable Safety Basis requirements are traceable from applicable Safety Analysis Reports. Some design elements that are used for testing or ease of operation are not traceable to safety base documents or requirements. Criteria is met CPP 651 PSD 4.8 Plant Safety Document Section 4.8 "Unirradiated Fuel Storage Facility" is the current documented safety analysis for the Unirradiated Fuel Storage Facility, CPP-651. Implemented threshold values are documented in W.O. 5817, Check Alarm and Set Points and Background Values. Safety basis requirements from PSD 4.8 are included in various CAS software requirements document. A System Design Description is being developed that will include the safety basis requirements for the CAS and other requirements in one document. CPP 603 PSD 4.12 Plant Safety Document "Irradiated Fuel Storage Facility" is the current documented safety analysis for the Unirradiated Fuel Storage Facility, CPP-603. Implemented threshold values, documented in W.O. 5818, , attachment 1, section 3.2, Check Alarm and Set Points and Background Values. Safety basis requirements from PSD 4.12 are included in various CAS software requirements document. A System Design Description is being developed that will include the safety basis requirements for the CAS and other requirements in one document
3. The design is correct, consistent, clearly presented, and feasible.	Criteria is partially met See above. Design is not clearly presented. This is being corrected through the development of System Design Descriptions for the CAS systems for both CPP-651 and CPP-603. It is recommended that issuing the in process System Description Documents be verified in a follow up assessment.

Software Design Description
Approach:

Review the appropriate documents, such as vendor specifications for I&C software design, description of the components and subcomponents of the software design, including databases and internal interfaces. The design may be documented in a standalone document such as an SDD or embedded in other documents. The SDD should contain the information listed below:

- A description of the major safety components of the software design as they relate to the I&C software requirements and any interactions with non-safety components.
- A technical description of the software with respect to control flow, control logic, mathematical model, and data structure and integrity.
- A description of the allowable or prescribed ranges for inputs and outputs.
- A description of error handling strategy and use of interrupt protocols.
- The design described in a manner suitable for translating into computer codes.

Note: In instances where software design documentation is not available, the contractor may be able to construct a design summary on the basis of available program documentation, review of the source code (if applicable), and information from the facility staff. Care should be taken to ensure that such a design summary is consistent with the complexity and importance of the software to the safety functions.

Topical Area: 3. Software Verification and Validation	Objective: The V&V process and related documentation for I&C software are defined and maintained to ensure that the software adequately and correctly performs all its intended functions; ensure that the software does not perform any adverse unintended function.
Criteria	Comments/Notes/ Results
1. All I&C software requirements and design have been verified and validated for correct operation using testing, observation or inspection techniques.	Criteria is met CAS systems for CPP-651 and CPP-603 have been in operation without system changes since 1998 and 1999, respectively. Both are calibrated quarterly. Calibration records for work orders 75884 and 758850 verify that the system works as designed.
2. Relevant abnormal conditions have been evaluated for mitigating unintended functions through testing, observation or inspection techniques.	Criteria is met CAS systems for CPP-651 and CPP-603 have been in operation without system changes since 1998. Both are calibrated quarterly. Calibration records for work orders 75884 and 758850 verify that the system works as designed.

Software Verification and Validation
Approach:

Review appropriate documents, such as test plans, test cases, test reports, system qualification plans and reports, and vendor qualification reports to determine if:

- An established process for validating the requirements exists.
- The V&V process includes an assessment to demonstrate whether the software requirements and system requirements are correct, complete, accurate, consistent, and testable.
- Dynamic testing has been performed to confirm time-dependent input-output relations, speed, recovery time, response time, frequency of reading input and updating output, throughput, and interrupt handling, as specified in the SRD.
- Each test case is executed in accordance with the test procedures and test plan.
- Correct inputs have been used for each test case.
- Sufficient number of tests has been executed to test all I&C software requirements.
- Tests representative of the anticipated application have been executed.
- Hardware and software configurations pertaining to the software V&V are specified.
- Results of V&V activities including test execution, observations, inspections and reviews are documented.
- V&V is complete and all unintended conditions are dispositioned before software is approved for use.
- Traceability exists from software requirements to design and testing, and, as appropriate, to user documentation.
- V&V is performed by individuals or organizations that have sufficient independence from the creation of I&C software.
- For SSCs that have been in operation for several years, the team should consider using an approach similar to an ANS 10.4 *a posteriori* review.

Topical Area: 4. Software User Documentation	Objective: Software documentation is available to guide the user in installing, operating, managing, and maintaining the I&C software.
Criteria	Comments/Notes/ Results
1. The system requirements and constraints, installation procedures, and maintenance procedures such as database fine-tuning are clearly and accurately documented.	Criteria is met The instructions for maintaining and updating the software build process are contained in PLN-1326, "Criticality Alarm System Computer Software Configuration Management Plan".
2. Any operational data system requirements and limitations are clearly and accurately documented.	Criteria is met Operating limits for the CAS software by itself are not formally documented. The software and hard ware have been treated as a single system. Operation limits are currently documented in TS 15B8 and completed work orders 5817 and 5818. It is expected that this will be more clearly defined in the to be issued System Design Descriptions for CPP-603 and CPP-651.
3. Documentation exists to aid the users in the correct operation of the software and to provide assistance for error conditions. Form 3019 http://xena/edm01i/4179/1044713.tif MCP-1170, http://xena/edm04a/10030/2507485.tif STD-101, http://xena/edm03g/9570/2392334.tif	Criteria is met Operation of the software is directed via menus contained in the software user interface.
4. Appropriate software design and coding documentation to assist in any future software modifications is defined and documented.	Not applicable. This system is nearing the end of its life cycle. See PLN-1326 section 2.1. The system has operated successfully, without modification since 1998. Changes will probably be a total change out of the hardware and software.

Software User Documentation
Approach:

The team will review the user's manual and related documents. These documents may exist either as a standalone documents or embedded in other documents. The user documentation should contain:

- User instructions that contain an introduction, a description of the user's interaction with the software, and a description of any required training necessary to use the software.
- Input and output specifications appropriate for the function being performed.
- A description of user messages or other indications as a result of improper input or system problems, and user response.
- Information for obtaining user and maintenance support.
- A description of system requirements and limitations such as operating system versions, minimum disk and memory requirements, and any known incompatibilities with other software.
- A description of any system requirements or limitations for operational data such as file sizes.
- Recommendations for routine database maintenance and instructions for performing this maintenance.
- Design diagrams, structure or flow charts, pseudo code, and source code listings necessary for performing future modifications of custom software.

Topical Area: 5. Software Configuration Management	Objective: Software components and products are identified, managed, and changes to those items are controlled.
Criteria	Comments/Notes/ Results
1. All software components and products to be managed are identified and controlled.	Criteria is met The software components are identified and controlled as configuration items in PLN-1326, "Criticality Alarm System Computer Software Configuration Management Plan". PLN-1326 was issued on 4/21/2004. There is insufficient history to verify implementation. A follow up assessment to verify implementation is recommended.
2. For those components and products procedures exist to manage the modification and installation of new versions.	Criteria is met PLN-1326, "Criticality Alarm System Computer Software Configuration Management Plan" is used to manage the modification and installation of all new software upgrades.
3. Procedures for modifications to those components and products are followed and controlled.	Criteria is partially met Modification to the system will be controlled using PLN-1326, "Criticality Alarm System Computer Software Configuration Management Plan". PLN-1326 was issued on 4/21/2004. There is insufficient history to verify implementation. A follow up assessment to verify implementation is recommended.

Software Configuration Management
Approach:

Review appropriate documents such as applicable procedures related to I&C software change control to determine if a software configuration management process exists and is effective. This determination is made based on the following actions.

- Verify the existence of a software configuration management plan, either in standalone form or embedded in another document.
- Verify that a configuration baseline is defined and that it is being adequately controlled. This baseline should include operating system components, any associated runtime libraries, acquired software executables, custom-developed source code files, users' documentation, the appropriate documents containing software requirements, software design, software V&V procedures, test plans and procedures, and any software development and quality planning documents.
- Review procedures governing change management for installation of new versions of the software components including new releases of acquired software.
- Review software change packages and work packages to ensure that:
  - possible impacts of software modifications are evaluated before changes are made,
  - various software system products are examined for consistency after changes are made,
  - software is tested according to established standards after changes have been made.
- Verify by sampling that documentation affected by software changes accurately reflects all safety-related changes that have been made to the software.

Interview a sample of cognizant line, engineering, Quality Assurance (QA) managers, and other personnel to verify their understanding of the change control process and commitment to manage changes affecting design, safety basis, and software changes in a formal, disciplined, and auditable manner.

Topical Area: 6. Software Quality Assurance	Objective: Software quality activities are evaluated for applicability to the I&C software, defined to the appropriate level of rigor, and implemented.
Criteria	Comments/Notes/ Results
1. Software quality activities and software practices for requirements management, software design, software configuration management, procurement controls, verification and validation including reviews and testing, and documentation have been evaluated and established at the appropriate level for proper applicability to the I&C software under assessment.	Criteria is met MCP-3630 and PLN-1326 establish this criterion.
2. The software quality activities have been effectively implemented.	Implementation has yet to be verified. PLN-1326 was issued on 4/21/2004. MCP-3630 was issued July 3, 2003. There has not been sufficient time to verify implementation. A follow up assessment to verify implementation is recommended.

Software Quality Assurance
Approach:

The team will confirm the existence of an SQA Plan, either as a standalone document or embedded in another document, and related procedures, QA assessment reports, test reports, problem reports, corrective actions, supplier control, and training, and determine the effectiveness of the SQA program. The assessment also entails interviewing managers, engineers, operators, and software users. The SQA Plan shall identify:

- The software products to which the Plan applies.
- The organizations responsible for maintaining software quality, along with their tasks and responsibilities.
- Required documentation such as SRD, SDD, V&V, SCM, and software user documentation.
- Supplier control provisions for meeting established requirements.
- Standards, conventions, techniques, or methodologies that guide software development and ensure compliance to the same.
- Methods for error reporting and corrective action.

Any tailoring or note of non-applicability of software quality activities.
Through the assessment of other topical areas, the effectiveness of implementing the software quality activities will be noted.

Topical Area: 7. Software Procurement	Objective: Acquired software meets the applicable level of software quality to ensure the safe operation of the system.
Criteria	Comments/Notes/ Results
1. Agreements for the acquisition of software programs or components identify the functional, operational and quality requirements appropriate for their use.	Criteria is met Purchase Order 21383808, 10/25/88 describes the desired system specifications. MCP-550 addresses purchasing software systems.
2. Acquired software is verified to meet the identified quality requirements.	Criteria is met Calibration records for work orders 75880 and 758850 verify that the system works as designed.

Software Procurement
Approach:

Vendors that supply COTS and other types of acquired software are evaluated to ensure that the software is developed under an appropriate quality assurance program and are capable of providing software that satisfies the specific requirements. The volume of commercial use for the vendor software, especially with COTS software, should be considered in determining the adequacy of the vendor's quality assurance program. The assessment of software procurements shall include the following:

Determine the existence of acquired software quality requirements. These requirements may be embedded in the DOE contractors' or subcontractors' procurement requirements or processes, software or system requirements description, software or system design description, or a software quality plan.

Review the methods used to verify that acquired software meets the specified quality requirements, and determine if these methods accomplish those requirements. These methods may be included in a software quality plan or software test plan.

Review evidence that the acquired software was evaluated for the appropriate level of quality. This evidence may be included in test results, a test summary, vendor site visit reports, or vendor quality program assessment reports.

Topical Area: 8. Software Problem Reporting and Corrective Action	Objective: A process for I&C software problem reporting is established, maintained, and controlled, including notification of errors, failures, and corrective action development.
Criteria	Comments/Notes/ Results
1. Documented practices and procedures for reporting, tracking, and resolving problems or issues are defined and implemented.	Criteria is met MCP-598 documents these processes. ORPS report 1998-0001 and ICARE #28147 document the implementation.
2. Organizational responsibilities for reporting issues, approving changes and performing corrective actions are identified and effective.	Criteria is met MCP-598 establishes processes for issue identification, reporting and verification of issue resolution. ORPS report ID--LITC-FUELRCSTR- 1998-0001 and ICARE #28990, action # #28147 are examples of implementation. Implementation of PLN-1326 establishes a process for approving system changes. PLN-1326 was issued on 4/21/2004. There is insufficient history to verify implementation. A follow up assessment to verify implementation is recommended.

Software Problem Reporting and Corrective Action
Approach:

Review documents and interview facility staff for the problem reporting and notification process to determine if:

- A formal procedure exists for software problem reporting and corrective action development that addresses software errors, failures, and resolutions.
- The problems that impact the operation of the software are promptly reported to affected organizations.
- Corrections and changes are evaluated for impact and approved prior to being implemented.
- Corrections and changes are verified for correct operation and to ensure no side effects were introduced.
- Preventive measures and corrective actions are provided to affected organization in a timely manner associated with the impact of the original defect.
- The organizations responsible for problem reporting and resolution are defined.